Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) An access privilege transferring method for safely transferring access privileges between ~~clients~~ clients, and between ~~the~~ clients and ~~servers~~ servers, over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a ~~network~~network, and ~~accessing~~ access to each of the objects complying with privilege information held by each of the clients is allowed, ~~comprising the steps of:~~ comprising:

~~(a) causing each of the clients to hold~~ holding user information and secret ~~information;~~ information by each of a plurality of clients;

~~(b) causing the server to hold the~~ holding, in a server, the user information and the secret information of at least a first of the plurality ~~each~~ of ~~the~~ clients;

~~(c) causing the client to generate~~ generating privilege ~~information;~~ information by the at least the first of the plurality of clients;

~~(d) causing the client to apply~~ applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information; by the at least the first of the plurality of clients;

~~(e) causing the client to transmit~~ transmitting the user information, the privilege information and the protected privilege information from the at least the first of the plurality of clients to ~~another client;~~ at least a second of the plurality of clients;

~~(f) causing the another client to transmit~~ retransmitting, from the at least the second of the plurality of clients, the user information, the privilege information and the protected privilege information to the server, thereby making a request to access ~~each~~ an object;

~~(g) causing the server to check to see~~ checking, by the server, whether the privilege information received from the at least the second of the plurality of clients ~~in Step (f)~~ is valid;

~~(h) causing the server to apply~~ applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege ~~information;~~ by the server;

~~(i) causing the server to compare~~ comparing the protected privilege information received by the server ~~in Step (f)~~ with the protected privilege information generated by the server; ~~in Step (h);~~ and

~~(j)~~ allowing ~~an~~ access to ~~each~~ an object in response to the coincidence of the received protected privilege information and the generated protected privilege information ~~two as a result of the comparison in Step (i).~~ based on the results of the comparison.

2. (Currently Amended) The access privilege transferring method according to claim 1, wherein the ~~another client transmits~~ at least the second of the plurality of clients retransmits the user information, the privilege information and the protected privilege information ~~received in Step (e)~~ to at least a third of the plurality of clients. ~~a second other client.~~

3. (Currently Amended) An access privilege transferring method for allowing each of the clients activated over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a

network and ~~accessing~~ access to each of the objects complying with privilege information held by each of the clients is ~~allowed,~~ allowed to safely transfer access privileges to another client, ~~comprising the steps of:~~ comprising:

~~(a)~~ holding user information and secret information to be shared by at least ~~the server(s);~~ one server;

~~(b)~~ generating privilege information; and

~~(c)~~ applying a predetermined calculating operation to information comprising at least the privilege information and the secret ~~information~~ information, ~~to~~ thereby ~~generate~~ generating protected privilege information ~~capable of being~~ to be safely transferred to ~~another~~ a client.

4. (Currently Amended) An access privilege transferring method for allowing each of the servers activated over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network and ~~accessing~~ access to each of the objects ~~following~~ based on privilege information held by each of the clients is ~~allowed,~~ allowed to safely respond to an access request issued from the client to which access privileges are transferred, ~~comprising the steps of:~~ comprising:

~~(f)~~ receiving an access request including user information, privilege information and protected privilege information;

~~(g)~~ checking ~~to see~~ whether the received privilege information ~~received in Step (f)~~ is valid;

~~(h)~~ applying a predetermined calculating operation to information comprising at least the privilege information and the secret ~~information to~~ information, thereby ~~generate~~ generating protected privilege information;

~~(i)~~ comparing the received protected privilege information ~~received in Step (f)~~ with the generated protected privilege ~~information generated in Step (h);~~ information; and

~~(j)~~ allowing ~~an~~ access to ~~each of the objects~~ an object in response to the coincidence of the ~~two~~ received protected privilege information and the generated protected privilege information based on the results of the comparison. ~~as a result of the comparison in Step (i).~~

5. (Currently Amended) The access privilege transferring method according to claim 1, wherein applying ~~the~~ a predetermined calculating operation ~~is to apply~~ further comprises applying a one-way function to a bit string obtained by concatenating operands with one another.

6. (Currently Amended) An access privilege transferring method for safely transferring access privileges between ~~clients~~ clients, and between ~~the~~ clients and ~~servers~~ servers, over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network and ~~accessing~~ access to each of the objects complying with privilege information held by each of the clients is allowed, ~~comprising the steps of:~~ comprising:

~~(A) causing each of the clients to hold~~ holding user information and secret ~~information;~~ information by each of a plurality of clients;

~~(B) causing the server to hold~~ holding, in a server, the user information and the secret information of ~~each of the clients;~~ at least a first of the plurality of clients;

~~(C) causing the client to generate~~ generating privilege ~~information;~~ information by the at least the first of the plurality of clients;

~~(D) causing the client to apply~~ applying a predetermined calculating operation to information comprising at least the privilege information and the secret information,

thereby generating first protected privilege ~~information;~~ information by the at least the first of the plurality of clients;

~~(E) causing the client to transmit~~ transmitting the user information, the privilege information and the first protected privilege information from the at least the first of the plurality of clients to ~~another client;~~ at least a second of the plurality of clients;

~~(F) causing the another client to receive~~ receiving, by the at least the second of the plurality clients, a challenge character string from the server;

~~(G) causing the another client to apply~~ applying the ~~a~~ predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information, thereby generating second protected privilege ~~information;~~ information by the at least the second of the plurality clients;

~~(H) causing the another client to transmit~~ transmitting the user information, the privilege information and the second protected privilege information from the at least the second of the plurality clients to the server, thereby making a request to access ~~each of the objects;~~ an object;

~~(I) causing the server to check to see~~ checking, by the server, whether the privilege information received by the server ~~in Step (H)~~ is valid;

~~(J) causing the server to apply~~ applying the ~~a~~ predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating first protected privilege ~~information;~~ information by the server;

~~(K) causing the server to apply~~ applying the ~~a~~ predetermined calculating operation to information comprising at least the challenge character string and the generated first protected privilege ~~information generated in Step (J);~~ information, thereby generating second protected privilege information;

~~(L) causing the server to compare~~ comparing the received second protected privilege information ~~received in Step (H)~~ with the generated second protected privilege ~~information generated in Step (K);~~ information; and

~~(M)~~ allowing ~~an~~ access to ~~each~~ the object in response to the coincidence of the ~~two~~ received second protected privilege information and the generated second protected privilege information ~~as a result~~ based on the results of the ~~comparison in Step (N).~~ comparison.

7. (Currently Amended) The access privilege transferring method according to claim 6, wherein the ~~another client transmits~~ at least the second of the plurality of clients retransmits the user information, the privilege information and the protected privilege information ~~received in Step (E) to a second other client.~~ at least a third of the plurality of clients.

8. (Currently Amended) An access privilege transferring method for safely transferring access privileges between clients and servers to which user information, privilege information and first protected privilege information are transferred, over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network and ~~accessing~~ access to each of the objects complying with privilege information held by each of the clients is allowed, ~~comprising the steps of:~~ comprising:

~~(F) causing the server to transmit~~ transmitting a challenge character string from the server to ~~the~~ a client that makes a request to access ~~each of the objects;~~ an object;

~~(G) causing the client to apply~~ applying a predetermined calculating operation to information comprising at least the challenge character string and ~~the~~ first protected privilege information, thereby generating second protected privilege ~~information;~~ information by the client;

~~(H) causing the client to transmit~~ retransmitting, by the client, ~~the~~ user information, the privilege information and the second protected privilege information to ~~the~~ a server, thereby making a request to access ~~each of the objects;~~ an object;

~~(I) causing the server to check to see~~ checking, by the server, whether the privilege information received by the server ~~in Step (H)~~ is valid;

~~(J) causing the server to apply~~ applying the ~~a~~ predetermined calculating operation to information comprising at least the privilege information and secret information, thereby generating first protected privilege ~~information;~~ information by the server.

~~(K) causing the server to apply~~ applying the ~~a~~ predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information generated by the server, ~~in Step (J),~~ thereby generating second protected privilege ~~information;~~ information by the server;

~~(L) causing the server to compare~~ comparing, in the server, the second protected privilege information received and checked by the server ~~in Step (H)~~ with the second protected privilege information generated by the server; ~~in Step (K);~~ and

~~(M) causing the server to allow an~~ allowing access to ~~each of the objects~~ an object by the server in response to the coincidence of the ~~two~~ received second protected privilege information and the generated second protected privilege information based on the results of the comparison. ~~as a result of the comparison in Step (N).~~

9. (Currently Amended) The access privilege transferring method according to claim 6, wherein applying ~~the~~ a predetermined calculating operation ~~is to~~ further comprises applying ~~apply~~ a one-way function to a bit string obtained by concatenating operands with one another.

10. (Currently Amended) An access privilege transferring method for safely transferring access privileges between ~~clients~~ clients, and between ~~the~~ clients and ~~servers~~

servers, over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network and ~~accessing~~ access to each of the objects complying with privilege information held by each of the clients is allowed, ~~comprising the steps of:~~ comprising:

~~(a) causing each of the clients to hold~~ holding user information and secret ~~information;~~ by each of a plurality of clients;

~~(b) causing the server to hold the~~ holding, in a server, the user information and the secret information of at least a first of the plurality ~~each~~ of ~~the~~ clients;

~~(c) causing the client to generate~~ generating privilege ~~information;~~ information by the at least the first of the plurality of clients;

~~(d) causing the client to encrypt~~ encrypting the generated privilege information by using the secret information, thereby generating protected privilege ~~information;~~ information by the at least the first of the plurality of clients;

~~(e) causing the client to transmit~~ transmitting, from the at least the first of the plurality of clients; the user information and the protected privilege information to ~~another client;~~ at least a second of the plurality of clients;

~~(f) causing the another client to transmit~~ retransmitting, by the at least the second of the plurality of clients, the user information and the protected privilege information to the server, thereby making a request to access ~~each of the objects;~~ an object;

~~(g) causing the server to decrypt~~ decrypting the protected privilege information by using the secret information corresponding to the user information, thereby generating privilege ~~information;~~ information by the server;

~~(h) causing the server to check to see~~ checking, by the server, whether the privilege information generated by the server ~~in Step (g)~~ is valid; and

~~(i)~~ allowing ~~an~~ access to ~~each~~ an object in accordance with the result of ~~check for~~ the validity ~~in Step (h).~~ check.

11. (Canceled)

12. (Currently Amended) An access privilege transferring method for allowing each of servers activated over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network and ~~accessing~~ access to each of the objects following privilege information held by each of the clients is ~~allowed,~~ allowed to safely respond to an access request issued from the client to which access privileges are transferred, ~~comprising the steps of:~~ comprising:

~~(f)~~ receiving an access request including user information and protected privilege information;

~~(g)~~ decrypting the protected privilege information by using secret information corresponding to the user information to thereby generate privilege information;

~~(h)~~ checking whether the generated privilege information ~~generated in Step (g)~~ is valid; and

~~(i)~~ allowing an access to ~~each of the objects~~ an object in accordance with the result of ~~check for validity in Step (h).~~ the validity check.

13. (Currently Amended) An access privilege transferring method for safely transferring access privileges between ~~clients~~ clients, and between ~~the~~ clients and ~~servers~~ servers, over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network and ~~accessing~~ access to each of the objects complying with privilege information held by each of the clients is allowed, ~~comprising the steps of:~~ comprising:

~~(A) causing each of the clients to hold~~ holding user information and secret ~~information;~~ information by each of a plurality of clients;

~~(B) causing the server to hold the~~ holding, in the server, the user information and the secret information of at least a first of the plurality ~~each~~ of ~~the~~ clients;

~~(C) causing the client to generate~~ generating privilege ~~information;~~ information by the at least the first of the plurality of clients;

~~(D) causing the client to encrypt~~ encrypting the generated privilege information by using the secret information, thereby generating first protected privilege ~~information;~~ by the at least the first of the plurality of clients;

~~(E) causing the client to transmit~~ transmitting the user information, the privilege information and the first protected privilege information from the at least the first of the plurality of clients to ~~another client;~~ at least a second of the plurality of clients;

~~(F) causing the another client to receive~~ receiving, by the at least the second of the plurality of clients, a challenge character string from the server,

~~(G) causing the another client to encrypt~~ encrypting the challenge character string by using the first protected privilege information, thereby generating second protected privilege ~~information;~~ information by the at least the second of the plurality of clients;

~~(H) causing the another client to transmit~~ retransmitting, by the at least the second of the plurality of clients, the user information, the privilege information and the second protected privilege information to the server, thereby making a request to access ~~each~~ an object;

~~(I) causing the server to check to see~~ checking, by the server, whether the privilege information received by the server ~~in Step (H)~~ is valid;

~~(J) causing the server to encrypt~~ encrypting the privilege information by using the secret information, thereby generating first protected privilege ~~information;~~ information by the server;

~~(K) causing the server to encrypt~~ encrypting the challenge character string by using the first protected privilege information generated by the server, ~~in Step (J),~~ thereby generating second protected privilege ~~information;~~ information by the server;

~~(L) causing the server to compare~~ comparing the received second protected privilege information ~~received in Step (H)~~ with the generated second protected privilege ~~information generated in Step (K);~~ information; and

~~(M)~~ allowing ~~an~~ access to ~~each~~ an object in response to the coincidence of the ~~two~~ received second protected privilege information and the generated second protected privilege information ~~as a result of the comparison in Step (N).~~ based on the results of the comparison.

14. (Currently Amended) An access transferring method for safely transferring access privileges between clients and servers to which user information, privilege information and first protected privilege information are transferred, over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network and ~~accessing~~ access to each of the objects complying with privilege information held by the client is allowed, ~~comprising the steps of:~~ comprising:

~~(F) causing the server to transmit~~ transmitting a challenge character string to the client that makes a request to access ~~each of the objects;~~ an object;

~~(G) causing the client to encrypt~~ encrypting the challenge character string by using the first protected privilege information, thereby generating second protected privilege information;

~~(H) causing the client to transmit~~ transmitting the user information, the privilege information and the second protected privilege information to ~~the~~ a server, thereby making a request to access ~~each of the objects;~~ an object;

~~(I) causing the server to check to see~~ checking whether the received privilege information ~~received in Step (H)~~ is valid;

~~(J) causing the server to encrypt~~ encrypting the privilege information by using secret information, thereby generating first protected privilege information;

~~(K) causing the server to encrypt~~ encrypting the challenge character string by using the generated first protected privilege ~~information generated in Step (J),~~ information, thereby generating second protected privilege information;

~~(L) causing the server to compare~~ comparing, in the server, the second protected privilege information received by the server ~~in Step (H)~~ with the second protected privilege information generated by the server; ~~in Step (K);~~ and

~~(M) causing the server to allow an~~ allowing access to ~~each of the objects~~ an object by the server in response to the coincidence of the ~~two as a result of the comparison in Step (N).~~ received second protected privilege information and the generated second protected privilege information based on the results of the comparison.

15. (Currently Amended) An information managing method for safely managing secret information between ~~clients and/or~~ clients, and between ~~the~~ clients and ~~servers~~ servers, over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network, ~~comprising the steps of:~~ comprising:

~~causing a first client to transmit~~ transmitting secret information from at least a first of a plurality of clients to at least a second ~~client;~~ of the plurality of clients;

~~causing the first client to transmit~~ transmitting an encryption key from the at least the first of the plurality of clients to the at least the second ~~client; and~~ of the plurality of clients;

~~causing the second client to encrypt~~ encrypting, by the at least the second of the plurality of clients, the secret information by using the encryption ~~key;~~ key; and ~~thereafter~~ storing the encrypted secret information, by the at least the second of the plurality of clients, in a secondary memory device.

16. (Currently Amended) An information managing method for safely managing secret information between ~~clients and/or~~ clients, and between ~~the~~ clients and ~~servers~~ servers, over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network, ~~comprising the steps of:~~ comprising:

~~causing a first client to encrypt the~~ encrypting secret information by using an encryption key, thereby generating protected secret ~~information;~~ information by at least a first of a plurality of clients;

~~causing the first client to transmit~~ transmitting the protected secret information from the at least the first of the plurality of clients to at least a second ~~client;~~ of the plurality of clients;

~~causing the second client to store~~ storing, by the at least the second of the plurality of clients, the received protected secret information in a secondary memory device;

~~causing the first client to transmit~~ transmitting a decryption key for decrypting the information encrypted by the encryption key from the at least the first of the plurality of clients to the at least the second ~~client;~~ of the plurality of clients; and

~~causing the second client to decrypt~~ decrypting, by the at least the second of the plurality of clients, the protected secret information by using the decryption key, thereby obtaining the secret information.

17. (Original) The information managing method according to claim 16, wherein the encryption key is identical to the decryption key.

18. (Currently Amended) An information managing method for safely managing secret information between ~~clients and/or~~ clients, and between ~~the~~ clients and ~~servers~~ servers, over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network, ~~comprising the steps of:~~ comprising:

~~causing a first client to transmit~~ transmitting secret information from at least a first of a plurality of clients to at least a second ~~client;~~ of a plurality of clients;

~~causing the second client to hold~~ holding, by the at least the second of the plurality of clients, an encryption key for encrypting information and a decryption key for decrypting the encrypted information encrypted by the encryption key;

~~causing the second client to transmit~~ transmitting the decryption key from the at least the second of the plurality of clients to the at least the first ~~client;~~ of the plurality of clients;

~~causing the second client to store~~ storing, by the at least the second of the plurality of clients, protected secret information obtained by encrypting the secret information with the encryption key in a secondary memory device; and

~~causing the second client to decrypt~~ decrypting the protected secret information by using the decryption key, thereby obtaining the secret ~~information.~~ information by the at least the second of the plurality of clients.

19. (Currently Amended) An information managing method for safely managing secret information between ~~clients and/or~~ clients, and between ~~the~~ clients and ~~servers~~ servers, over an object space in which at least one server for providing objects and at least one client ~~for~~ requiring the objects are connected to one another by a network, ~~comprising the steps of:~~ comprising:

~~causing a first client to transmit~~ transmitting ~~first~~ secret information from at least a first of a plurality of clients to at least a second ~~client;~~ of the plurality of clients;

~~causing the second client to transmit~~ transmitting, by the at least the second of the plurality of clients, a challenge character string to the at least the first ~~client;~~ of the plurality of clients;

~~causing the first client to apply~~ applying a predetermined calculating operation to the challenge character string and ~~second~~ the secret information, thereby generating an encryption ~~key;~~ key by the at least the first of the plurality of clients;

~~causing the first client to transmit~~ transmitting the encryption key from the at least the first of the plurality of clients to the at least the second ~~client;~~ of the plurality of clients; and

~~causing the second client to store~~ storing, by the at least the second of the plurality of clients, protected secret information obtained by encrypting the secret information by using the encryption key in a secondary memory device.